Performance-based Work Statement for
Naval Education and Training Command (Code N53)
Program Analytical Services in support of
Ready Relevant Learning Program Office
28 March 2018

1. Introduction

The Office of the Deputy Chief of Naval Operations (OPNAV) Manpower, Personnel, Training, & Education (MPT&E; N1) Division is located in Arlington, VA. N1's mission is to anticipate Navy warfighting needs, identify associated personnel capabilities, and recruit, develop, manage, and deploy those capabilities in an agile, cost-effective manner.

The Naval Education and Training Command (NETC) is a subordinate command to N1 that is responsible for training, education and professional development of the Navy's 400,000 active duty and reserve Sailors through accession, continuing education, and advancement training. NETC is located in Pensacola, Florida. NETC is an Echelon II command.

NETC Code N53 is the Ready, Relevant Learning (RRL) Program Office, which supports innovative efforts to provide Sailors with the right training at the right time throughout their career long learning continuum. It is one of the primary pillars of the Navy's Sailor 2025 initiative.

2. Background

The centerpiece of the NETC mission is the progressive transformation of Sailors from civilians to a ready force of disciplined warriors with the technical, ethical, and leadership skills necessary to fight and win. The NETC N53 RRL Program Office supports three major lines of effort: Career Long Learning Continuum, Modern Delivery at Point of Need, and Integrated Content Development. RRL will be executed in three phases: Block Learning, Enhanced Accessible, Learning, and Anytime, Anywhere Learning.

2.1 Federal Holidays

The contractor will normally not provide services on the following federal holidays: New Year's Day, Martin Luther King Day, President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, and Christmas Day. When a holiday occurs on a Saturday, federal employees are normally granted the previous Friday as the holiday observance period. When a holiday occurs on a Sunday, federal employees are normally granted the following Monday as the holiday observance period. There are occasions when the FRC East reduces operations in conjunction with the following holidays: Thanksgiving Day, Christmas Day, and New Year's Day, which encompass additional non-holiday work days and weekends. When such a notice is given, the contractor shall modify its support level for the reduced operations.

2.2 Installation Closure

In the event that an unforeseen installation closure occurs on a regular work day, the Contracting Officer's Representative (COR) will have the option to reschedule the work on any day that is mutually satisfactory to the contractor and the PCO. Additionally, when said closure occurs, personnel shall secure material, equipment, vehicles, and buildings, as determined by assigned NETC headquarters personnel, in accordance with current Naval Air Station Pensacola Instruction (NASPCOLAINST) 3440.4D Destructive Weather, 5500.1J Antiterrorism Force

. Protection/Physical Security Plan procedures for the preservation and protection of the property.

2.3 Severe Weather Closure
In the event of closings due to severe weather or other hazardous situations, notification to contractor employees to take appropriate actions will be given through the following website: https://www.cnic.navy.mil/regions/cnrse/installations/nas_pensacola/about/instructions.html. Information on the website will also include closing and delay bulletins and severe weather phone numbers.

2.4 Government Documents

Document Number	Document Title and/or Description
22 CFR, Parts 120-130	Foreign Relations, Chapter 1 Department of State, Subchapter M, International Traffic in Arms Regulations
29 CFR 1910.147	The control of hazardous energy (lockout/tag out)
DFARS 252.211-7003	Item Identification and Valuation (Aug 2008)
DFARS 252.227-7013	Rights In Technical Data - Noncommercial Items (Nov 1995)
DFARS 252.227-7014	Rights In Noncommercial Computer Software And Noncommercial Computer Software Documentation (Jun 1995)
FAR, Part 2.101	Definitions
FAR 52.204-9	Personal Identity Verification of Contractor Personnel
FAR 52.222-54	Employment Eligibility Verification
NIST SP 800-44	Guidelines on Securing Public Web Servers
	U.S. Office of Personnel Management (OPM) Final Credentialing Standards for Issuing Personal Identity Verification
21 CFR 1040	Code of Federal Regulations (CFR), Title 21, Part 1040, Performance Standards for Light-Emitting Products
29 CFR 1910	Occupational Safety and Health Standards (OSHS)

- *Copies of the CFR sections can be obtained from http://www.pmddtc.state.gov/regulations_laws/itar_offical.html.*
- *Copies of U.S. Code can be obtained from https://ile-help.nko.navy.mil/ile/content/policy/section508.aspx.*
- *Copies of DFARS clauses can be obtained from http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/dfars252_227.htm*
- *Copies of CFR documents can be obtained from http://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR*
- *Copies of FAR clauses can be obtained from http://farsite.hill.af.mil/vffara.htm.*
- *http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml.*
- *Copies of OPM document can be obtained from http://www.opm.gov/investigate/resources/index.aspx.*

Table 1: Government Documents

3. Scope

The contractor shall provide program analytical and management services, and subject matter expertise in the areas of metrics and analysis, training modernization and optimization, R&D/S&T and innovation efforts, training effectiveness assessment and NETC strategic communication and planning in support of Navy leadership initiatives such as Block Learning, Ready, Relevant Learning, Sailor 2025, and MPT&E Transformation. One of the critical focus areas is in measuring and improving training effectiveness. The contractor shall support the Navy in carrying out the mission

of optimizing the process of measuring training effectiveness to rapidly improve training and provide the Fleet with mission-capable Sailors. To accomplish this effort, the contractor shall manage and collaborate with diverse teams consisting of internal and external stakeholders and team-members.

4. Tasks

4.1. MPTE Program Management Support

4.1.1. Program and Project Management

- Provide program and project planning support using strategic tools (project portfolio management, etc.) in support of Sailor 2025; Ready, Relevant Learning; Block Learning; and MPTE Transformation.
- Develop performance monitoring metrics and data collection approaches, and identify business process improvements and efficiencies.
- Facilitate the development and execution of the NETC Science and Technology (S&T), Research and Development, and Innovation Plans
- Facilitate the implementation of new learning science techniques and technologies
- Present information to senior leadership.
- Manage and execute the Training Assessment Framework project under the Testing Modernization initiative.
- Manage and execute transformation timelines and projects.

4.1.2. Program and Policy Analysis

- Analyze implementation decisions (SECNAV, CNO, CNP, etc.) on the future learning state of the NETC organization and how these projects integrate with the NETC Strategic Plan.
- Research new or improved training technologies to modernize and optimize training under the Ready, Relevant Learning framework approved by CNO.
- Provide metric support via the automation of data capture and analysis throughout the domain.
- Analyze policy documents in a variety of different areas pertaining to Navy training.
- Analyze alternatives to improve training efficacy.

4.1.3. Analysis and assessment of the Navy's recruiting, manpower, personnel, training, and education strategic initiatives

- Analyze and evaluate the effectiveness of the programs listed in 4.1.1 (first bullet)
- Develop procedures and systems for establishing, operating, and assessing the effectiveness of the programs.
- Provide risk assessments.
- Facilitate research and analytic teams to evaluate studies on the effectiveness of training, training technology, training innovation and training processes in support of the programs.
- Integrate the POM process and draft funding requests to initiate and execute projects to improve training and management outcomes.
- Execute the NETC Training Effectiveness in support of the programs.
- Execute R&D studies and training modernization projects

4.1.4. Strategic Management

- Assist with strategic planning on organizational transformation initiatives.
- Provide subject matter expertise on the integration of future Learning Assessment System requirements into RRL Learning Stack and future projects within the NETC Strategic Plan.
- Track strategic goals and subsets.

4.1.5. Visual Communications and Social Media

Not applicable

4.2. Financial Administration and Compliance

Not applicable

4.3. POM Analysis

Not applicable

4.4. Administrative Support

- Maintain NETC N53 internal branch Current Projects Underway slide deck to track RRL and related MPTE transformation projects.
- Maintain NETC N53 Modernized Delivery Project schedule, Plan of Actions and Milestones (POAM), and other tracking reports required by internal and external stakeholders.
- Plan and track annual budget expenditures.

5. Other Pertinent Information

5.1. Acronyms

Not applicable

5.2. Period of Performance—

The period of performance is 15 September 2018 through 14 September 2021.

5.3. Place of Performance—

The primary place of performance is NETC Headquarters, 250 Dallas St. Pensacola, FL 32508-5220.

material handling equipment/trucks for the duration of this contract. The contractor shall maintain the assigned space in a neat and orderly manner. Contractor shall only use government-furnished facilities and equipment to accomplish the tasks required under this contract. Personal or company use of phones, utilities, computers, printers, copiers, etc., not directly related to required services is strictly prohibited. Contractor shall not remove any government equipment or supplies from the worksite without the express written permission of the COR or his/her designated representative.

The Government will provide access to NMCI computer workstations, NMCI email accounts, telephone, and fax service for contractor personnel. The NMCI seats for all personnel will be standard workstations or laptops.

Facilities: Contractor personnel supporting NETC will be located in NETC headquarters, 250 Dallas St., Pensacola, FL, 32508-5220, or within a 30-mile radius of NETC headquarters in the event of an emergency relocation.

Access to Business Sensitive Information: The Government will provide access to information as necessary. Contractor personnel shall sign a non-disclosure agreement prior to obtaining access to business sensitive information.

5.6.1 Standards of Conduct

The contractor shall not employ any person whose employment under the contract could in any way result in a conflict of interest with the mission of the NETC. All personnel employed by the contractor in the performance of this effort, or any agent of the contractor entering the government installation shall obey all regulations of the installation and NETC. The contractor shall be responsible for employee competency and conduct and for taking disciplinary actions with respect to its employees. The removal from the job site of contractor personnel shall not relieve the contractor of the requirement to provide personnel to perform the specified tasks outlined in this SOW. The government reserves the right to deny access to the NETC to contractor employees, if the employee's presence would be detrimental to the NETC's mission, or performance of work in this SOW. The government reserves the right to require removal of any contractor employee from the job site, if said employee endangers personnel, property or mission. In such cases, the COR will advise the contractor of the reason for requesting removal of an employee, or for withdrawal of authorization for the employee to enter the installation.

5.6.2 Work Attire

Contractor employees shall maintain a standard of grooming and personal appearance IAW NETC's business casual work environment. The prime contractor's company name must be identified on the outer garment and shall be distinguishable from NETC employees. The shirt shall have sleeves and be clean, neat, and fit properly. Subcontractor employees shall wear the uniform of the prime contractor, and may, under the prime contractor's company name, list the subcontractor's name. Company identification shall be displayed on the outer garment and affixed permanently (e.g., sewed, embroidered, or inked). All costs associated with the purchase, maintenance, and laundering of uniforms will be at the contractor's expense.

5.6.3 Contractor Administrative Control and Supervision

Contractor employees shall be under the administrative control and supervision of designated contractor supervisors, site leads, and relief supervisors, and shall perform the tasks prescribed herein. Additionally, the contractor shall select, supervise, and exercise control and direction over their subcontractors under the contract. The contractor shall not supervise, direct, or control the activities of Navy personnel or the employees of any other contractor (other than their subcontractors). The

material handling equipment/trucks for the duration of this contract. The contractor shall maintain the assigned space in a neat and orderly manner. Contractor shall only use government-furnished facilities and equipment to accomplish the tasks required under this contract. Personal or company use of phones, utilities, computers, printers, copiers, etc., not directly related to required services is strictly prohibited. Contractor shall not remove any government equipment or supplies from the worksite without the express written permission of the COR or his/her designated representative.

The Government will provide access to NMCI computer workstations, NMCI email accounts, telephone, and fax service for contractor personnel. The NMCI seats for all personnel will be standard workstations or laptops.

Facilities: Contractor personnel supporting NETC will be located in NETC headquarters, 250 Dallas St., Pensacola, FL, 32508-5220, or within a 30-mile radius of NETC headquarters in the event of an emergency relocation.

Access to Business Sensitive Information: The Government will provide access to information as necessary. Contractor personnel shall sign a non-disclosure agreement prior to obtaining access to business sensitive information.

5.6.1 Standards of Conduct

The contractor shall not employ any person whose employment under the contract could in any way result in a conflict of interest with the mission of the NETC. All personnel employed by the contractor in the performance of this effort, or any agent of the contractor entering the government installation shall obey all regulations of the installation and NETC. The contractor shall be responsible for employee competency and conduct and for taking disciplinary actions with respect to its employees. The removal from the job site of contractor personnel shall not relieve the contractor of the requirement to provide personnel to perform the specified tasks outlined in this SOW. The government reserves the right to deny access to the NETC to contractor employees, if the employee's presence would be detrimental to the NETC's mission, or performance of work in this SOW. The government reserves the right to require removal of any contractor employee from the job site, if said employee endangers personnel, property or mission. In such cases, the COR will advise the contractor of the reason for requesting removal of an employee, or for withdrawal of authorization for the employee to enter the installation.

5.6.2 Work Attire

Contractor employees shall maintain a standard of grooming and personal appearance IAW NETC's business casual work environment. The prime contractor's company name must be identified on the outer garment and shall be distinguishable from NETC employees. The shirt shall have sleeves and be clean, neat, and fit properly. Subcontractor employees shall wear the uniform of the prime contractor, and may, under the prime contractor's company name, list the subcontractor's name. Company identification shall be displayed on the outer garment and affixed permanently (e.g., sewed, embroidered, or inked). All costs associated with the purchase, maintenance, and laundering of uniforms will be at the contractor's expense.

5.6.3 Contractor Administrative Control and Supervision

Contractor employees shall be under the administrative control and supervision of designated contractor supervisors, site leads, and relief supervisors, and shall perform the tasks prescribed herein. Additionally, the contractor shall select, supervise, and exercise control and direction over their subcontractors under the contract. The contractor shall not supervise, direct, or control the activities of Navy personnel or the employees of any other contractor (other than their subcontractors). The

government will not exercise any supervision or control over the contractor employees in performance of contractual services under the contract, and the contractor is accountable to the government for the actions of contractor personnel.

5.6.4 Supervisory Authority
The contractor is responsible for delegating team lead and supervisory authority to its workforce members in order to manage the work and internal QA responsibilities. Therefore, the contractor shall designate one person onsite to act as the primary site supervisor, and shall identify delegated team leads and supervisors to NETC COR and applicable TOCORs within one working day of changes. Team leads and supervisors shall assume several administrative duties and responsibilities, to include but not limited to: daily verification of hours worked and tasks assigned. All contractor supervisors shall be considered key personnel.

5.7. Security Requirements

Work under this contract is UNCLASSIFIED. The contractor shall comply with all applicable DOD and installation security regulations and procedures during the performance of this contract.

5.7.1 Security
The security requirements specified herein shall apply to the contractor and subcontractors. The contractor shall comply with applicable on-site security regulations related to government installation and facility access.

5.7.1.1 Classified Processing and Access to Classified Systems
The contractor shall safeguard classified information and meet the security requirements identified in the DD Form 254. The contractor shall enforce these safeguards throughout the life of the contract including the transport and delivery phases.

5.7.1.2 Operations Security (OPSEC)
The contractor shall develop, implement, and maintain an OPSEC program to protect controlled unclassified and classified activities, information, equipment, and material used or developed by the contractor and any subcontractor during performance of the contract. Guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring are provided in NIST SP 800-37. This program may include Cybersecurity and Communications Security (COMSEC). The OPSEC program shall be in accordance with National Security Decision Directive (NSDD) 298. If the contractor does not have an established OPSEC Plan that addresses the protection of, critical information, sensitive, proprietary, or controlled unclassified information, the Government will provide a template for the Contractor's internal development of an OPSEC Plan. Additional OPSEC program planning guidance can be found in DI-MGMT-80934C, OPERATIONS SECURITY (OPSEC) PLAN and NAVAIR OPERATIONS SECURITY (OPSEC) REQUIREMENTS (attachment). The OPSEC program, at a minimum, shall include:

a) Assignment of responsibility for OPSEC direction and implementation

b) Issuance of procedures and planning guidance for the use of OPSEC techniques to identify vulnerabilities and apply applicable countermeasures

c) Establishment of OPSEC education and awareness training to include Basic OPSEC training, produced by the Interagency OPSEC Support Staff (IOSS), which can be found at https://www.iad.gov/ioss/department/opsec-fundamentals-course-opse1300-opse1301-opse1300e-10045.cfm (OPSE1301 OPSEC Fundamentals)

d) Provisions for management, annual review, and evaluation of OPSEC programs

e) Flow down of OPSEC requirements to subcontractors when applicable

5.7.1.3 Unclassified Contractor-Owned Network Security - Safeguarding of Unclassified Controlled Technical Information

The safeguarding of Controlled Unclassified Technical Information applies to prime contractors and their subcontractors (if applicable) for information resident on or transiting through contractor unclassified information systems. The contractor shall provide security to safeguard unclassified controlled technical information on their unclassified information systems from unauthorized access and disclosure. The contractor shall take means (defense-in-depth measures) necessary to protect the confidentiality, integrity, and availability of Government controlled unclassified information.

(1) The contractor shall manage and maintain contractor-owned unclassified IT network assets used to process U.S. Government controlled unclassified information (sensitive information) IAW FAR 252.204-7012,

(A) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or

(B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and

(2) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of FAR 252.204-7012, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability

5.7.1.4 Cyber Incident and Compromise Reporting

The contractor shall report to DoD certain cyber incidents that affect unclassified controlled technical information resident on or transiting contractor unclassified information systems set forth IAW FAR 252.204-7012. The contractor shall also provide the report to the NAWCTSD Contracting Officer, NAWCTSD Security Manager, and the NAWCTSD Information Systems Security Manager (ISSM).

5.7.1.5 Access to DoD Installations, Government Information, and Information Technology (IT) Systems - Personnel Security Background Checks

a) The Common Access Card (CAC) shall be the principal identity credential for supporting interoperable access to DoD installations, facilities, buildings, controlled spaces, and access to U.S. Government information systems IAW FAR 52.204-9. The Contractor shall coordinate with the appropriate NAWCTSD Technical Point of Contact (TPOC), Contracting Officer Representative (COR), government sponsor, and NAWCTSD Security Office Trusted Agents for issuance of the CAC via the Trusted Associate Sponsorship System (TASS) Program. More information for obtaining the CAC can be found at http://www.cac.mil/common-access-card/getting-your-cac/for-contractors/.

b) Contractor personnel whom do not have a security clearance, but require a CAC in performance of their sensitive duties (including access to controlled unclassified information, but not access classified information), shall coordinate with the NAWCTSD Security Office to complete a National Agency Check with Local Agency Checks including Credit Check (NACLC/TIER- 3) background investigation, which includes submission of fingerprints and the Standard Form SF-86 (Questionnaire for National Security Positions). The contractor shall submit the Standard Form 86 to the NAWCTSD Security Office for processing. There shall be no additional NACLC/TIER-3 submissions for contractors holding a valid national security clearance. The Government may issue the credential upon favorable return of the Federal Bureau of Investigations (FBI) fingerprint check, pending final favorable completion of the NACLC/TIER-3.

c) Access to restricted areas, controlled unclassified information or Government Information Technology by contractor personnel shall be limited to those individuals who have been determined trustworthy as a result of the favorable completion of a NACLC/TIER-3R or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, a NACLC/TIER 3 shall be conducted and favorably reviewed by the appropriate DoD component, agency, or activity prior to permitting such access.

d) The contractor shall comply with the Cybersecurity and personnel security requirements for accessing U.S. Government IT systems specified in the contract. The contractor shall review and become familiar with the credentialing standards presented in OPM Memorandum for Issuing Personal Identity Verification cards to use as an aid in their employee selection process. The NAWCTSD Security Office will apply the credentialing standards and execute the credentialing process for individual contractors.

5.7.1.6 Personnel Security – Background Checks

Contractor personnel shall undergo the company internal vetting process prior to gaining access to U.S. Government controlled unclassified information. To comply with immigration law, the contractor shall use the Employment Eligibility Verification Program (E-Verify) IAW FAR 52.222-54.

5.7.1.7 International Traffic and Arms Regulation

The contractor shall ensure that foreign persons, as defined under section 120.16 of the International Traffic and Arms Regulation (ITAR) (22 CFR, Parts 120 – 130), are not given access to U.S. Government controlled unclassified information, sensitive information, defense articles, defense

services, or technical data, as defined in the ITAR, Part 120, without proper issuance of an export license from the U.S. Government authority.

5.7.1.8 Personnel Security – Reporting of Adverse or Derogatory Information related to Contractors

The Contractor shall report to the NAWCTSD Security Office adverse or derogatory information pertaining to on-site CSS personnel (when applicable) or contractor personnel in direct support of this contract. Information reported to the Government Contracting Agency shall be integrated and reported in Contractor Performance Assessment Reporting System (CPARS) on contractor performance of PERsonnel SECurity (PERSEC) related aspects of contractor performance.

a) Adverse or derogatory information reporting of contractor personnel. Example: Domestic Violence arrest, or other violent or sexual crime arrest or self-report.
b) When contractor personnel receive a revocation of an Interim or denial for the issuance of a CAC until final adjudication
c) When a denial or suspension of clearance occurs for a contractor employee
d) When contractor employee receives a final denial of eligibility for a security clearance.

5.7.1.9 Government-Issued Personal Identification Credentials

The contractor and subcontractor(s) (when applicable) shall account for all forms of U.S Government-provided identification credentials (CAC or U.S. Government-issued identification badges) issued to the contractor (or their employees in connection with performance) under the contract. The contractor shall return such identification credentials to the issuing agency at the earliest of any of the circumstances listed below, unless otherwise determined by the U.S. Government. The contracting officer may delay final payment under the contract if the contractor or subcontractor fails to comply with these requirements.

a) When no longer needed for contract performance.

b) Upon completion of the contractor employee's employment.

c) Upon contract completion or termination

5.7.1.10 Contractor "Out-processing" Policy

The contractor and subcontractor(s) (when applicable) shall have in place (established and enforced) an "out-processing" policy for employees that leave the company, including suspension of account access, return of all PCs, laptops, smartphones, and other electronic devices (Government-furnished IT equipment and contractor-issued IT equipment) that contain U.S. Government Controlled Unclassified Information. The contractor shall also ensure that out-processed employees receive debriefings on the need to maintain confidentiality of U.S. Government Controlled Unclassified Information.

5.7.1.11 Supply Chain Risk Management (SCRM) For National Security Systems

The Contractor shall mitigate supply chain risk in the provision of supplies and services to the Government per FAR 252.239-7018, Supply Chain Risk, and CNSSD -505, Supply Chain Risk Management (SCRM). The contractor shall, implement a process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing

mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal.

5.7.1.12 Protection of Critical Program Information (CPI)

a. When applicable, the Contractor shall identify candidate CPI and Resident CPI which requires protection IAW DoDI 5200.39. The CPI identified shall be approved by the USG Program Manager. The CPI identification shall include a review of the system, unique integration, support equipment and the Non-Resident design/process/material aspects of the program. All identified CPI shall be protected with appropriate countermeasures.

b. When applicable, the Contractor shall develop a Program Protection Implementation Plan (PPIP) to include all requirements outlined in the Government provided PPP. The PPIP shall be used as a focal point for the Contractor's Program Security efforts. The PPIP is derived from the PPP and should not restate what is written in the PPP but rather address specifically how the Contractor will implement Program Protection. The Contractor shall plan for and implement countermeasures which mitigate foreign intelligence collection, technology exploitation, supply chain threats, and system vulnerabilities relative to the protection of CPI, CC, and CUI. (CDRL PPP001, Program Protection Implementation Plan, DI-MGMT-81826)

c. When applicable, the Contractor shall ensure each Contractor/ Sub-Contractor employee supporting this contract completes Contractor developed and conducted Program Protection awareness training in Contractor format; (a) prior to performing any contract/task order work, and (b) completes annual refresher course training throughout the period of performance. This training is specific to the protection of CPI and tailored to each facility handling, storing, processing CPI.

5.7.1.13 Transmission of Controlled Unclassified Information (CUI) via e-mail

The Contractor shall use approved encryption to safeguard the electronic transmission of all Controlled Unclassified Information. The Contractor shall ensure that when transmitting CUI over non-secure e-mail (e.g. not connected to the Navy Marine Corps Intranet through Broadband Unclassified Remote Access System / Virtual Private network), those transmissions are encrypted using Department of Defense Public Key Infrastructure (PKI), or an approved DoD External Certificate Authority, in accordance with Public Key Infrastructure & Public Key Enabling, DoDI 8520.02, 24 May 2011.

5.7.1.14 Transmission of Controlled Unclassified Information (CUI) via S.A.F.E.

Safe Access File Exchange (SAFE). SAFE is designed to provide an alternative way to send encrypted files other than email. Information regarding the use of SAFE can be found at https://safe.amrdec.army.mil/safe/Default.aspx. The contractor shall ensure the following:

a. All files transferred via SAFE shall be for official US Government related business.
b. All files transferred via SAFE shall be UNCLASSIFIED.
c. SAFE **CANNOT** be used to transmit classified information
d. All files shall be encrypted.

5.7.2 Cybersecurity

The contractor shall deliver NETC Authority To Operate (ATO) cybersecurity documentation for training content products. The contractor shall deliver NAWCTSD ATO cybersecurity documentation for other products.

5.7.2.1 Cybersecurity for training content products

The contractor shall deliver NETC ATO accreditation documentation for training content products.

5.7.2.2 Cybersecurity for other products

The contractor shall deliver a security architecture for the training product that satisfies the DODI 8510.01 Risk Management Framework (RMF) security control set as defined in NIST SP 800-53 for a CNSSI 1253 Security Categorization of an NSS as (Confidentiality= Low), (Integrity=Low), (Availability=Low).

5.7.2.3 Cybersecurity Compliance

a. The contractor shall assess and verify that the application software functions as designed in a secured operating system environment and is free of elements that might be detrimental to the secure operation of the resource operating system, as described in NIST SP 800-53, Rev 4 and in the STIGs.

b. The contractor shall perform an assessment of the software against the Cybersecurity compliant operating system using the Secure Content Automation Protocol (DISA/SCAP) Content and Tools.

5.7.2.3.1 Cybersecurity Control Considerations

a. The contractor shall design, develop, document, integrate, verify, and deliver an application that satisfies the Cybersecurity controls as defined in NIST SP 800-53, Rev 4, Chapter 2.

b. The contractor shall verify that the software meets the security controls specified in NIST SP 800-53, Rev 4, Chapter 3, for a System Category (Confidentiality, High – Integrity, Low – Availability, Low).

5.7.2.3.2 Cybersecurity Certification and Accreditation Support

a. The contractor shall comply with the Cybersecurity Assessment process IAW DODI 8510.01, Enclosure 5.

b. The contractor shall participate with Information System Security Officer to complete Application Security and Development Checklists.

5.7.2.3.3 Cybersecurity and Personnel Security Requirements for Accessing Government IT Systems - Credentialing Standards

The contractor shall comply with the Cybersecurity and personnel security requirements for accessing U.S. Government IT systems specified in the contract. Authorization to Operate

The contractor shall prepare the Authorization to Operate (ATO) Package IAW the CDRL.

5.7.2.4 Software Integrity Testing and Certification

The contractor shall test and certify that the training product applications software are designed to function in a properly secured operating system environment and is free of elements that might be detrimental to the secure operation of the resource operating system, as described in NIST SP 800-53 . The contractor shall provide a Vendor Compliance Test Report for Software (VCTRS) for the contractor developed software applications IAW the ATO Package CDRL. Commercial Item software does not require a VCTRS.

5.7.2.5 Information Assurance Vulnerability Management Program (IAVMP)

The contractor shall incorporate the applicable DoD and DoN IAVMP messages issued through Contractor Government Final Inspection (CGFI) for training product components. The contractor shall document the unincorporated IA Vulnerability Alerts (IAVAs), IA Vulnerability Bulletins (IAVBs), and IA Vulnerability Technical Advisories (IAVTAs) in the ATO Package (Plan of Actions and Milestones) POA&M. The contractor shall provide justification for each unincorporated IAVMP message (i.e., describe the specific negative impact the IAVMP message incorporation would have on training product operation). The contractor shall document the information resulting from this task in the ATO Package cited above. The contractor shall document this information in the Plan of Action and Milestones (POA&M) tab of the package cited above. The contractor shall use the DoD-authorized assessment tools to perform IAVA compliance validation and verification (e.g. ACAS and SCAP Tool).

5.7.2.6 Cybersecurity On-site Training

The contractor shall provide 8 hours of Cybersecurity training for the on-site System Administrator and designated Cybersecurity representatives designated for the training product. The contractor shall provide the training within 30 days after the Ready-For-Training (RFT) date, as specified in the contract, for a maximum of eight Government-designated personnel. The Cybersecurity training course shall provide Government designated personnel the necessary skills to maintain the required level of Cybersecurity posture in order to ensure continued certification of the system. The contractor shall use the ATO Package Cybersecurity System Administrator Guide (SAG) as the primary support reference document during the Cybersecurity training course.

5.7.2.6.1 Cybersecurity Training & Certification

The contractor shall provide Cybersecurity equipped personnel per the following (DFARS 252.239-7001):

a. The contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform Cybersecurity functions in accordance with DoD 8570.01-M, Cybersecurity Workforce Improvement Program. The contractor shall meet the applicable information assurance certification requirements, including:
(1) DoD-approved Cybersecurity workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and
(2) Appropriate operating system certification for Cybersecurity technical positions as required by DoD 8570.01-M.
b. Upon request by the Government, the contractor shall provide documentation supporting the Cybersecurity certification status of personnel performing Cybersecurity functions.

c. The contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing Cybersecurity functions.

5.8. Travel—

Travel may be required in support of tasks identified by the PCO or COR. All required CONUS and OCONUS travel shall be approved by the COR or TOCOR in advance. Travel and per diem costs incurred in the replacement of personnel will not be reimbursed when such replacement is accomplished at the contractor's or employee's convenience.
Contract will include up to 5 trips annually.

5.9. Other Direct Costs (ODCs)—

None.

5.10. Other Information—

5.10.1. All contractor personnel shall wear the government-issued CAC as an identification badge. Contractor personnel shall identify themselves as contractor employees when attending meetings, answering Government telephones, sending e-mails, or working in situations where their actions could be construed as acts of Government officials.

5.10.2. Whenever granted access to sensitive information, contractor employees shall follow applicable DoD/DON instructions, regulations, policies and procedures when reviewing, processing, producing, protecting, destroying and/or storing that information. Operational Security (OPSEC) procedures and practices must be implemented by both the contractor and contract employee to protect the product, information, services, operations and missions related to the contract. The contractor shall designate an employee to serve as the Contractor's Security Representative. The Contractor's Security Representative shall be the primary point of contact on any security matters.

5.10.3. No data provided to, or developed by, the contractor shall be used for any purpose other than the tasks assigned. All information (data files and hard copy) becomes the property of the Government and the contractor shall return them at the completion of the task. The Government shall not be required to pay royalties, recurring license fees, use tax or similar additional payments for any contractor-developed product or associated software presentations.

5.10.4. The Contractor shall not disclose and must safeguard business sensitive and procurement sensitive information, computer systems and data, Privacy Act Data, and government personnel work products that are obtained or generated in the performance of this contract. The contractor shall safeguard all sensitive (including For Official Use Only (FOUO) and Privacy Act and critical program information and comply with SECNAVINST M-5510.30. The contractor shall enforce these safeguards throughout the life of the contract.

5.10.5. The contractor shall comply with Privacy Act and DOD Privacy Act Program for protecting unauthorized disclosure of personal information. The contractor must adhere to the Privacy Act, Title 5 of the U.S. Code-Section 552a and applicable agency rules and regulations referenced at http://privacy.navy.mil/. The contractor shall ensure that employees assigned to this effort understand and adhere to the Privacy Act regulations. The contractor shall identify and safeguard reports and data accordingly.

5.10.6. All contractor employees shall be fully trained prior to performing the work defined in the PWS. The contractor shall provide employees training to maintain currency with emergent technologies. Contract personnel will be expected to complete annual training specifically identified in this PWS or as identified by the COR in support of Navy policy for maintaining a safe and secure workplace such as Prevention of Sexual Harassment (POSH) training, Level I Anti-Terrorism Awareness Training, and Automated Information Security Annual Training and maintain records of completion. These training requirements are estimated to be 12 hours per year and can be completed during the normal work hours electronically through Navy Knowledge Online or similar electronic portals.

6. List of Deliverables

PWS	Deliverable	Recipient	Level of Inspection	Frequency
All	Kick-off Meeting	Gov't Stakeholders	100% by attendees	10 days after award
All	Monthly Status Reports	COR	100% by Recipient	NLT the 15th of each month
4.1.1	NETC N53 Quarterly updates	COR	100% by Recipient	NLT the first date of each fiscal quarter
4.1.1	Bi-weekly Senior Leadership Briefs	COR	100% by Recipient	2 Business days before each presentation
4.1.4	Updates to NETC Strategic Plan –Annual Update	COR	100% by Recipient	NLT 1 Sept. of each year
4.4	Updates to the Current Projects Underway slide deck	COR	100% by Recipient	NLT the 15th day of each month

The purpose of the kick-off meeting is to discuss technical and contracting objectives of the PWS, milestone schedules for deliverables, and methodologies and tools for accomplishing performance tasks.

The Contractor shall prepare a monthly progress report to include (a) summary of actions taken and progress made, and disposition of any outstanding problems and issues, and (b) a review of work planned for the next month to meet task requirements.

The contractor shall prepare all reports, documents or briefings required for performance per DoD/DON and local guidance. All reports shall contain suitable markings as contractor prepared and should be delivered in Word or Power Point format and submitted electronically to the Government Contracting Officer Representative (COR) for review and acceptance within the periods identified by specific project assignments. Contractor shall provide Word compatible electronic copy with all hard copies.

The Government will have 10 calendar days to review deliverables. The COR will have the right to reject or require correction of any deficiencies found in the deliverables that do not conform to government requirements. In the event of rejection of a deliverable, the Contractor will be notified in writing by the COR of the specific reasons why the deliverable is being rejected. The Contractor will meet with the COR to discuss/review if necessary. The Contractor shall have 7 calendar days to correct the rejected deliverable and return it to the COR.

7. Performance Standards

Performance Element	Performance Requirement	Surveillance Method	Frequency	Acceptable Quality Level
Contract Deliverables	Contract deliverables furnished as prescribed in the PWS, attachments, CDRLs, etc., as applicable.	Inspection by the COR	100% inspection of all contract deliverables.	>95% of deliverables submitted timely and without rework required.
Overall Contract Performance	Overall contract performance of sufficient quality to earn a Satisfactory (or higher) rating in the COR's annual report on Contractor Performance	Assessment by the COR	Annual	All performance elements rated Satisfactory (or higher)
Invoicing	Monthly invoices per contract procedures are timely and accurate.	Review & acceptance of the invoice	Monthly	100% accuracy

8. Points of Contact (POC)

Contracting Officer Representative (COR)
NETC N53, RRL Program Office

Mr. Marion Conley
250 Dallas Street, Code N536
Pensacola, FL 32508-5220
850-452-6076
marion.conley@navy.mil

Contracting Officer

9. Enterprise-wide Contractor Manpower Reporting Application (ECMRA)

The contractor shall report contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for **NETC** via a secure data collection site. Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

(1) W, Lease/Rental of Equipment;
(2) X, Lease/Rental of Facilities;
(3) Y, Construction of Structures and Facilities;
(4) D, Automatic Data Processing and Telecommunications, IT and Telecom- Telecommunications Transmission (D304) and Internet (D322) ONLY;
(5) S, Utilities ONLY;
(6) V, Freight and Shipping ONLY.

The contractor is required to completely fill in all required data fields using the following web address https://doncmra.nmci.navy.mil.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://doncmra.nmci.navy.mil.